

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁
JAPAN PATENT OFFICE

1c979 U.S. PTO
10/079405
02/22/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 4月27日

出 願 番 号

Application Number:

特願2001-132253

出 願 人

Applicant(s):

富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 6月 7日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3053620

【書類名】 特許願

【整理番号】 0140160

【提出日】 平成13年 4月27日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明の名称】 パケット転送装置、半導体装置、および、パケット転送システム

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市幸区堀川町 6 6 番地 2 富士通エルエス
 アイソリ्यूション株式会社内

 【氏名】 長友 晃彦

【発明者】

 【住所又は居所】 神奈川県川崎市幸区堀川町 6 6 番地 2 富士通エルエス
 アイソリ्यूション株式会社内

 【氏名】 浅野 和也

【発明者】

 【住所又は居所】 神奈川県川崎市幸区堀川町 6 6 番地 2 富士通エルエス
 アイソリ्यूション株式会社内

 【氏名】 橋田 淳一

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100092152

 【弁理士】

 【氏名又は名称】 服部 毅巖

 【電話番号】 0426-45-6644

【手数料の表示】

【予納台帳番号】 009874

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705176

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット転送装置、半導体装置、および、パケット転送システム

【特許請求の範囲】

【請求項 1】 複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とするパケット転送装置。

【請求項 2】 前記制御情報は、パケットに対するフィルタリング処理の有無を示し、

前記処理手段は、前記制御情報がフィルタリングが必要であることを指示している場合には、当該パケットを破棄する、

ことを特徴とする請求項 1 記載のパケット転送装置。

【請求項 3】 外部のネットワークに接続された入出力ポートを有し、

前記処理手段は、前記外部のネットワークに接続された入出力ポートから入力されたパケットが、内部のネットワークのアドレス情報を有している場合には、これをフィルタリングすることを特徴とする請求項 2 記載のパケット転送装置。

【請求項 4】 前記制御情報は、前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報であり、

前記処理手段は、前記制御情報に基づいて、指定された入出力ポートから当該パケットを出力する、

ことを特徴とする請求項 1 記載のパケット転送装置。

【請求項 5】 前記テーブルには、異なる階層に属する複数のヘッダ情報と、当該複数のヘッダ情報に対応する制御情報とが対応付けて格納されていることを特徴とする請求項 1 記載のパケット転送装置。

【請求項 6】 前記制御情報取得手段によって、複数のテーブルから複数の制御情報が 1 つのパケットに対して取得された場合には、前記処理手段が実際に実行すべき処理を決定する処理決定手段を更に有することを特徴とする請求項 1 記載のパケット転送装置。

【請求項 7】 前記制御情報は、パケットに対するフィルタリングの有無を示し、

前記処理決定手段は、前記複数のテーブルから複数の制御情報が取得された場合に何れか 1 つの制御情報がフィルタリングが必要であることを指示している場合には、当該パケットを破棄する、

ことを特徴とする請求項 6 記載のパケット転送装置。

【請求項 8】 前記制御情報は、前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報であり、

前記処理決定手段は、前記複数のテーブルから複数の制御情報が取得された場合には、最も階層が高いヘッダ情報を含むテーブルから取得された制御情報によって指定される入出力ポートから当該パケットを出力する、

ことを特徴とする請求項 6 記載のパケット転送装置。

【請求項 9】 複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とする半導体装置。

【請求項 1 0】 複数のネットワークがパケット転送装置によって接続され、それぞれのネットワーク間でパケットを転送するパケット転送システムにおいて、

前記パケット転送装置は、

複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とするパケット転送システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明はパケット転送装置および半導体装置に関し、特に、複数の入出力ポートから入力されたパケットを該当する入出力ポートに転送するパケット転送装置、半導体装置、および、パケット転送システムに関する。

【 0 0 0 2 】

【従来の技術】

近年、インターネットの普及により、一般家庭やいわゆる S O H O (Small Office Home Office) でもアクセスルータが使用されつつある。

【 0 0 0 3 】

現在、主に使用されているアクセスルータは、I S D N (Integrated Service Digital Network) ルータと呼ばれるものであり、インターネットにアクセスす

るWAN (Wide Area Network) 側の帯域は64Kbpsのインターフェースを有し、家庭側やSOHO側は帯域10Mbpsのイーサネットのインターフェースを複数有するものが一般的である。

【0004】

ところで、近年では、CATV (Cable Television)、ADSL (Asymmetric Digital Subscriber Line)、および、FTTH (Fiber To The Home) 等のブロードバンドと呼ばれる通信サービスが台頭してきた。これらは、WAN側の帯域が1Mbps以上であり、中には100Mbpsを越える広帯域を提供するサービスも存在する。一方、家庭内またはSOHO内でも、マルチメディアデータを送受信する必要性から、今後、100Mbpsクラスの帯域が要求される可能性がある。

【0005】

図17は、従来のアクセスルータの一例を示す図である。

この図に示すように、従来のアクセスルータは、レイヤ2 (データリンク層) スイッチ10、および、CPU (Central Processing Unit) 20によって構成されている。

【0006】

ここで、レイヤ2スイッチ10は、入出力ポート11~13、MAC (Media Access Control) ブロック14~16、スイッチブロック17、および、参照ブロック18によって構成されている。

【0007】

入出力ポート11~13は、例えば、WANやホストに接続され、これらとの間で情報を授受する。

処理手段14~16は、入出力ポート11~13によって受信されたパケットから宛先MACアドレスを抽出して参照ブロック18に供給し、出力すべき入出力ポートを特定する。そして、スイッチブロック17に対してそのパケットを供給し、特定された入出力ポートから出力させる。

【0008】

図18 (A) は、処理手段14の詳細な構成例を示している。この図に示すよ

うに、処理手段 1 4 は、参照ブロックインターフェース 1 4 a、スイッチブロックインターフェース 1 4 b、および、ヘッダ情報抽出回路 1 4 cによって構成されている。

【 0 0 0 9 】

参照ブロックインターフェース 1 4 a は、参照ブロック 1 8 との間のインターフェースである。

スイッチブロックインターフェース 1 4 b は、スイッチブロック 1 7 との間のインターフェースである。

【 0 0 1 0 】

ヘッダ情報抽出回路 1 4 c は、パケットからヘッダ情報（宛先 M A C アドレス）を抽出する。

なお、処理手段 1 4 ～ 1 6 は、同様の構成とされているので、処理手段 1 5、1 6 の説明は省略する。

【 0 0 1 1 】

図 1 7 に戻って、参照ブロック 1 8 は、処理手段 1 4 ～ 1 6 から供給された宛先 M A C アドレスから、出力すべき入出力ポートを特定する。

図 1 8 （ B ） は、参照ブロック 1 8 の詳細な構成例を示す図である。この図に示すように、参照ブロック 1 8 は、参照テーブル 1 8 a および比較回路 1 8 b によって構成されている。

【 0 0 1 2 】

参照テーブル 1 8 a は、図 1 9 に示すように、参照フィールドとデータフィールドから構成されている。参照フィールドには宛先 M A C アドレスが格納されており、また、データフィールドには該当する入出力ポートのポート番号が格納されている。

【 0 0 1 3 】

比較回路 1 8 b は、処理手段 1 4 ～ 1 6 から供給された宛先 M A C アドレスと、参照テーブルの参照フィールドとを比較し、該当する M A C アドレスが存在する場合には、対応するデータフィールドから制御情報であるポート番号を取得し、要求を行った処理手段に対して供給する。

【 0 0 1 4 】

CPU 2 0 は、ルーティング処理を実行する場合に、パケットのヘッダの変更やCRC (Cyclic Redundancy Check) コードの再計算等の処理を実行する。

次に、以上の従来例の動作について説明する。仮に、入出力ポート 1 1 がポート番号 # 1 であり、入出力ポート 1 2, 1 3 がそれぞれポート番号 # 2, # 3 であるとする。また、入出力ポート 1 1 および入出力ポート 1 2 は、ホストに接続されており、入出力ポート 1 3 はWANに接続されているとする。

【 0 0 1 5 】

このような場合において、入出力ポート 1 1 に接続されているホストから入出力ポート 1 2 に接続されているホストに向けてパケットが送信されたとする。

すると、入出力ポート 1 1 は、ホストから送信されたパケットを入力し、処理手段 1 4 に供給する。

【 0 0 1 6 】

処理手段 1 4 のヘッダ情報抽出回路 1 4 c は、パケットから宛先MACアドレスを抽出する。いまの例では、入出力ポート 1 2 に接続されているホストのMACアドレスであるMACアドレス # 2 が取得される。

【 0 0 1 7 】

このようにして抽出された宛先MACアドレスは、参照ブロックインターフェース 1 4 a を介して参照ブロック 1 8 に供給される。

参照ブロック 1 8 の比較回路 1 8 b は、取得した宛先MACアドレスと、参照テーブル 1 8 a の参照フィールドとを比較する。その結果、宛先MACアドレスであるMACアドレス # 2 は第 2 番目の項目と一致することから、比較回路 1 8 b は、対応するポート番号 # 2 を取得し、要求を行った処理手段 1 4 に供給する。

【 0 0 1 8 】

処理手段 1 4 は、参照ブロックインターフェース 1 4 a を介してポート番号を取得し、この取得したポート番号をパケットとともにスイッチブロックインターフェース 1 4 b を介してスイッチブロック 1 7 に供給する。

【 0 0 1 9 】

スイッチブロック 17 は、内蔵されたバッファにパケットを一時的に格納した後、当該パケットを、特定されたポート番号 # 2 に対応する処理手段 15 に供給する。

【0020】

処理手段 15 のスイッチブロックインターフェースは、スイッチブロック 17 から供給されたパケットを受信し、入出力ポート 12 を介してホストに供給する。

【0021】

以上の動作により、パケットをホスト間で転送することが可能になる。

【0022】

【発明が解決しようとする課題】

図 17 に示すような従来のアクセスルータの場合では、ハードウェアであるレイヤ 2 スイッチ 10 によって処理できるのは、文字通りレイヤ 2 に属する情報のレベルである。従って、それ以外の高度な判断を伴う処理（例えば、フィルタリング処理）を実現するためには、CPU 20 が処理を分担する必要がある。

【0023】

また、前述したように、近年では通信速度が高速化していることから、それに伴って、CPU 20 にかかる負担も増大する傾向にある。その結果、前述のような高度な処理を実行しようとする、CPU 20 が過負荷になり、場合によっては処理が追いつかずにパケットが消失する場合が発生するという問題点があった。

【0024】

本発明はこのような点に鑑みてなされたものであり、CPU 等の中央制御装置の負担を増大することなく高度な処理を実行するとともに、通信速度の高速化にも対応することが可能なパケット転送装置および半導体装置を提供することを特徴とする。

【0025】

【課題を解決するための手段】

本発明では上記課題を解決するために、図 1 に示す、複数の入出力ポート 1 a

～1 c と、前記複数の入出力ポート 1 a ～1 c のそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段 1 e と、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブル 1 g と、前記ヘッダ情報抽出手段 1 e によって抽出されたヘッダ情報に対応する制御情報を前記テーブル 1 g から取得する制御情報取得手段 1 f と、前記制御情報取得手段 1 f によって取得された制御情報に基づいて、パケットを処理する処理手段 1 d と、を有することを特徴とするパケット転送装置 1 が提供される。

【0026】

ここで、入出力ポート 1 a ～1 c は、パケット転送装置 1 に接続された他の装置との間でパケットを授受する。ヘッダ情報抽出手段 1 e は、複数の入出力ポート 1 a ～1 c のそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出する。テーブル 1 g は、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶している。制御情報取得手段 1 f は、ヘッダ情報抽出手段 1 e によって抽出されたヘッダ情報に対応する制御情報をテーブル 1 g から取得する。処理手段 1 d は、制御情報取得手段 1 f によって取得された制御情報に基づいて、パケットを処理する。

【0027】

また、複数の入出力ポートと、前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、を有することを特徴とする半導体装置が提供される。

【0028】

ここで、複数の入出力ポートは、半導体装置の外部に接続された他の装置との

間でパケットを授受する。ヘッダ情報抽出手段は、複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの3層（ネットワーク層）以上に属するヘッダ情報を抽出する。テーブルは、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶する。制御情報取得手段は、ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報をテーブルから取得する。処理手段は、制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する。

【 0 0 2 9 】

また、図1に示す、複数のネットワークがパケット転送装置によって接続され、それぞれのネットワーク間でパケットを転送するパケット転送システムにおいて、複数の入出力ポート1 a～1 cと、前記複数の入出力ポート1 a～1 cのそれぞれから入力されたパケットより、ネットワークプロトコルの3層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段1 eと、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブル1 gと、前記ヘッダ情報抽出手段1 eによって抽出されたヘッダ情報に対応する制御情報を前記テーブル1 gから取得する制御情報取得手段1 fと、前記制御情報取得手段1 fによって取得された制御情報に基づいて、パケットを処理する処理手段1 dと、を有することを特徴とするパケット転送システムが提供される。

【 0 0 3 0 】

ここで、入出力ポート1 a～1 cは、パケット転送装置1に接続された他の装置との間でパケットを授受する。ヘッダ情報抽出手段1 eは、複数の入出力ポート1 a～1 cのそれぞれから入力されたパケットより、ネットワークプロトコルの3層（ネットワーク層）以上に属するヘッダ情報を抽出する。テーブル1 gは、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶している。制御情報取得手段1 fは、ヘッダ情報抽出手段1 eによって抽出されたヘッダ情報に対応する制御情報をテーブル1 gから取得する。処理手段1 dは、制御情報取得手段1 fによって取得された制御情報に基づいて、パケットを処理する。

【 0 0 3 1 】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して説明する。

図1は、本発明の動作原理を説明する原理図である。この図に示すように、本発明のパケット転送装置1は、入出力ポート1a～1c、処理手段1d、ヘッダ情報抽出手段1e、制御情報取得手段1f、および、テーブル1gによって構成されている。

【0032】

ここで、入出力ポート1a～1cは、外部に接続されている装置との間でパケットを授受する。

ヘッダ情報抽出手段1eは、入出力ポート1a～1cから入力されたパケットから、ネットワークプロトコルの2層（データリンク層）および3層（ネットワーク層）以上に属するヘッダ情報を抽出する。

【0033】

テーブル1gは、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶している。

制御情報取得手段1fは、ヘッダ情報抽出手段1eによって抽出されたヘッダ情報に対応する制御情報をテーブル1gから取得する。

【0034】

処理手段1dは、制御情報取得手段1fによって取得された制御情報に基づいて、パケットを処理する。

次に、以上の原理図の動作について説明する。

【0035】

仮に、入出力ポート1aは、WANに接続されており、入出力ポート1bは、WEBサーバに、また、入出力ポート1cは、クライアントに接続されているとする。

【0036】

このような場合、WEBサーバについては、所定のTCPポート番号以外は、アクセスを禁止することが望ましい場合がある。その実現例を以下に説明する。

いま、入出力ポート1aからパケット2が入力されたとする。なお、このパケ

ット 2 は、入出力ポート 1 b に接続された W E B サーバに対して宛てられたものであり、アクセスが禁止されているポート番号を宛先 T C P ポート番号として含んでいるとする。

【 0 0 3 7 】

入出力ポート 1 a から入力されたパケット 2 は、ヘッダ情報抽出手段 1 e によってヘッダが抽出される。この例では、4 層に属する T C P ヘッダが抽出され、制御情報取得手段 1 f に供給される。

【 0 0 3 8 】

制御情報取得手段 1 f は、ヘッダ情報抽出手段 1 e によって抽出されたヘッダ情報に対応する制御情報をテーブル 1 g から取得する。

ここで、テーブル 1 g には、4 層に属する T C P ヘッダと制御情報とが関連付けて格納されており、制御情報取得手段 1 f には、ヘッダ情報抽出手段 1 e から供給されたヘッダ情報に対応する制御情報が制御情報取得手段 1 f に返される。

【 0 0 3 9 】

いまの例では、アクセスが禁止されている宛先 T C P ポート番号を含んでいるので、テーブル 1 g から取得された制御情報には、そのパケットをフィルタリング（廃棄）することが指示されている。

【 0 0 4 0 】

このような制御情報は、処理手段 1 d に供給される。処理手段 1 d は、制御情報取得手段 1 f から供給された制御情報に基づいて、入出力ポート 1 a から入力されたパケットを、出力先として指定された入出力ポート 1 b には供給せずに廃棄する。

【 0 0 4 1 】

以上の処理によれば、ネットワークの 4 層に属する情報に基づいてパケットをフィルタリングすることが可能になる。

次に、図 2 を参照して本発明の実施の形態について説明する。

【 0 0 4 2 】

図 2 は、本発明の実施の形態の構成例を示す図である。この図において、本発明のパケット転送装置 4 0 は、通信装置 4 1 を介してインターネット 4 2 に接続

されるとともに、ホスト 4 3, 4 4 に接続されている。

【0 0 4 3】

ここで、パケット転送装置 4 0 は、ホスト 4 3, 4 4 およびインターネット 4 2 に接続された他のホストとの間で情報を授受する。

通信装置 4 1 は、モデム等によって構成されており、例えば、公衆網を介してインターネット 4 2 に接続する際に、パケット転送装置 4 0 からのデジタルデータをアナログデータに変換するとともに、公衆回線からのアナログ信号をデジタル信号に変換する。

【0 0 4 4】

ホスト 4 3, 4 4 は、例えば、WEB サーバおよび POP サーバ等によってそれぞれ構成されている。

図 3 は、パケット転送装置 4 0 の詳細な構成例を示す図である。

【0 0 4 5】

この図に示すように、パケット転送装置 4 0 は、レイヤ 2 スイッチ 1 0、および、CPU 2 0 によって構成されている。

ここで、レイヤ 2 スイッチ 1 0 は、入出力ポート 1 1 ~ 1 3、処理手段 3 0 ~ 3 2、スイッチブロック 1 7、および、テーブル 3 3 によって構成されている。

【0 0 4 6】

ここで、入出力ポート 1 1 ~ 1 3 は、それぞれ、通信装置 4 1、ホスト 4 3、および、ホスト 4 4 に接続されており、これらとの間でパケットを授受する。

処理手段 3 0 ~ 3 2 (図 1 7 の MAC ブロックに対応) は、入出力ポート 1 1 ~ 1 3 によって受信されたパケットから宛先 MAC アドレス、IP アドレス、および、TCP ポート番号等のレイヤ 2 ~ レイヤ 4 に属するヘッダ情報を抽出し、テーブル 3 3 に供給し、そのパケットに対してなすべき処理の指定を受ける。

【0 0 4 7】

図 4 (A) は、処理手段 3 0 の詳細な構成例を示す図である。この図に示すように、処理手段 3 0 は、2 層ヘッダ情報抽出回路 3 0 a、3 層ヘッダ情報抽出回路 3 0 b、4 層ヘッダ情報抽出回路 3 0 c、参照ブロックインターフェース 3 0 d、および、スイッチブロックインターフェース 3 0 e によって構成されている。

【 0 0 4 8 】

2 層ヘッダ情報抽出回路 3 0 a は、入出力ポート 1 1 から供給されたパケットから 2 層ヘッダ情報を抽出する。

3 層ヘッダ情報抽出回路 3 0 b は、入出力ポート 1 1 から供給されたパケットから 3 層ヘッダ情報を抽出する。

【 0 0 4 9 】

4 層ヘッダ情報抽出回路 3 0 c は、入出力ポート 1 1 から供給されたパケットから 4 層ヘッダ情報を抽出する。

参照ブロックインターフェース 3 0 d は、テーブル 3 3 との間のインターフェースである。

【 0 0 5 0 】

スイッチブロックインターフェース 3 0 e は、スイッチブロック 1 7 との間のインターフェースである。

なお、処理手段 3 0 ～ 3 2 は、全て同様の構成とされているので、処理手段 3 1, 3 2 の説明は省略する。

【 0 0 5 1 】

テーブル 3 3 (図 1 7 の参照ブロック 1 8 に対応) は、処理手段 3 0 ～ 3 2 のそれぞれから供給された 2 層～ 4 層ヘッダ情報に基づいて対象となるパケットをどのように処理すべきかを決定する。

【 0 0 5 2 】

図 4 (B) は、テーブル 3 3 の詳細な構成例を示す図である。この図に示すように、テーブル 3 3 は、比較回路 3 3 a、連結比較回路 3 3 b、および、参照テーブル 3 3 c ～ 3 3 e によって構成されている。

【 0 0 5 3 】

比較回路 3 3 a は、各処理手段から供給された単一のヘッダ情報と、参照テーブルの参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドから制御情報を取得し、要求を行った処理手段に供給する。

【 0 0 5 4 】

連結比較回路 3 3 b は、各処理手段から供給された複数のヘッダ情報を適宜連結して得られた情報と、参照テーブルの参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドから制御情報を取得し、要求を行った処理手段に供給する。

【 0 0 5 5 】

図 5 は、連結比較回路 3 3 b の詳細な構成例を示す図である。この図に示すように、連結比較回路 3 3 b は、情報連結回路 5 0、参照情報レジスタ 5 1 ～ 5 3、出力ポート情報セクタ 5 4、および、フィルタ情報セクタ 5 5 によって構成されている。

【 0 0 5 6 】

情報連結回路 5 0 は、各処理手段から供給されたヘッダ情報（2 層～4 層のヘッダ情報）を各参照テーブルに応じて適宜連結し、参照情報レジスタ 5 1 ～ 5 3 に対して出力する。

【 0 0 5 7 】

参照情報レジスタ 5 1 ～ 5 3 は、情報連結回路 5 0 によって連結されたヘッダ情報を取得し、一時的に格納するとともに、参照テーブル 3 3 c ～ 3 3 e に供給する。

【 0 0 5 8 】

出力ポート情報セクタ 5 4 は、参照テーブル 3 3 c ～ 3 3 e からバス 6 0 を介して供給された制御情報のうち、出力ポートを示す情報である出力ポート情報を取得する。そして、出力ポート情報が複数存在する場合には、最も高い層のヘッダ情報を含むテーブルに対応する出力ポート情報を選択し、要求を行った処理手段に供給する。

【 0 0 5 9 】

フィルタ情報セクタ 5 5 は、参照テーブル 3 3 c ～ 3 3 e からバス 6 0 を介して供給された制御情報のうち、フィルタの有無を示すフィルタ情報を取得する。そして、フィルタ情報が複数存在する場合には、これらの何れか 1 つでもフィルタ処理が“有”になっていれば、フィルタ処理が必要である旨を、要求を行った処理手段に通知する。

【 0 0 6 0 】

参照テーブル 3 3 c ~ 3 3 e は、図 6 に示すように、参照フィールドとデータフィールドから構成され、参照フィールドには 2 層 ~ 3 層に属するヘッダ情報が適宜組み合わされたものが格納されている。この図の例では、参照フィールドには、3 層に属する送信元 I P アドレスおよび宛先 I P アドレスと、4 層に属する送信元 T C P ポート番号および宛先 T C P ポート番号とが格納されている。

【 0 0 6 1 】

データフィールドには、入出力すべきポートを指定する出力ポート情報と、フィルタの有無を示すフィルタ情報とが格納されている。

具体的には、例えば、第 1 行目に格納された情報の場合、送信元 I P アドレスが S A # 1 であり、宛先 I P アドレスが D A # 1 であり、送信元 T C P ポート番号が S P # 1 であり、宛先 T C P ポート番号が D P # 1 である場合には、入出力ポートは P # 1 であり、また、フィルタ処理は不要（無）である。

【 0 0 6 2 】

なお、参照テーブル 3 3 c ~ 3 3 e にはそれぞれ異なるテーブルが格納されており、これらの情報は外部から必要に応じて書き換えることができる。

次に、以上の実施の形態の動作について説明する。

【 0 0 6 3 】

最初に、図 7 に示すテーブルが、例えば、参照テーブル 3 3 c に格納されている場合に、図 8 に示すパケット # 1 およびパケット # 2 がインターネット 4 2 からパケット転送装置 4 0 に入力された場合の動作について説明する。なお、図 8 に示す 2 つのパケットは、宛先 T C P ポート番号のみが異なっており、その他は同一である。

【 0 0 6 4 】

先ず、パケット # 1 がパケット転送装置 4 0 に入力されると、入出力ポート 1 1 を介してパケットが取り込まれ、処理手段 3 0 に供給される。

処理手段 3 0 では、2 層ヘッダ情報抽出回路 3 0 a、3 層ヘッダ情報抽出回路 3 0 b、および、4 層ヘッダ情報抽出回路 3 0 c が、パケット # 1 からそれぞれ 2 層 ~ 4 層のヘッダ情報を抽出する。具体的には、パケットには、図 9 に示すよ

うに、2層ヘッダ、3層ヘッダ、および、4層ヘッダが順に格納されている。2層ヘッダは宛先MACアドレスおよび送信元MACアドレスによって構成され、3層ヘッダは宛先IPアドレスおよび送信元IPアドレスによって構成され、また、4層ヘッダは宛先TCPポート番号および送信元TCPポート番号によって構成されている。なお、図の空白部分には、他のヘッダの情報が格納されている。

【0065】

いまの例では、2層ヘッダ情報抽出回路30aは、宛先MACアドレス“ma#1”および送信元MACアドレス“max”を抽出し、3層ヘッダ情報抽出回路30bは、送信元IPアドレス“gax”および宛先IPアドレス“ga#1”を抽出し、また、4層ヘッダ情報抽出回路30cは、送信元TCPポート番号“x”および宛先TCPポート番号“80”を抽出する。

【0066】

2層ヘッダ情報抽出回路30a～4層ヘッダ情報抽出回路30cによって抽出された2層～3層ヘッダ情報は、参照ブロックインターフェース30dを介してテーブル33に供給される。

【0067】

いまの例では、参照テーブル33cには、図7に示す、複数のヘッダ情報を含むテーブルが格納されているので、テーブル33では、連結比較回路33bが対応するヘッダ情報を連結した後、参照テーブル33cに格納されている参照フィールドと、ヘッダ情報とを比較する。

【0068】

即ち、連結比較回路33bの情報連結回路50は、処理手段30から供給された2層～4層のヘッダ情報を取得し、3層および4層のヘッダ情報を抽出して連結した後、入力された入出力ポートのポート番号を更に連結し、参照情報レジスタ51に供給する。

【0069】

参照情報レジスタ51は、情報連結回路50から供給された3層および4層のヘッダ情報および受信した入出力ポートの情報を一時的に格納するとともに参照

テーブル 3 3 c に供給する。

【 0 0 7 0 】

参照テーブル 3 3 c は、参照情報レジスタ 5 1 から供給されたヘッダ情報と、参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドに格納されている制御情報を取得し、バス 6 0 を介して、出力ポート情報は出力ポート情報セクタ 5 4 に、また、フィルタ情報はフィルタ情報セクタ 5 5 に供給する。

【 0 0 7 1 】

いまの例では、パケット # 1 のヘッダ情報および入力された入出力ポートとは、図 7 に示す参照テーブルの第 1 行目の項目と一致するので、データフィールドから出力ポート情報として“CPU”が、また、フィルタ情報として“無”が取得され、“CPU”は出力ポート情報セクタ 5 4 に、また、“無”はフィルタ情報セクタ 5 5 に供給される。なお、図 7 において“gaany”および“tcpany”は任意の IP アドレスおよび TCP ポート番号を示している。

【 0 0 7 2 】

ここで、参照テーブル 3 3 c 以外の参照テーブルからの情報は存在しないので、出力ポート情報セクタ 5 4 およびフィルタ情報セクタ 5 5 は、出力ポート情報“CPU”およびフィルタ情報“無”を、要求を行った処理手段 3 0 に供給する。

【 0 0 7 3 】

処理手段 3 0 は、参照ブロックインターフェース 3 0 d を介してこれらの情報を受信する。そして、フィルタ情報は“無”であることから、フィルタ処理は不要であることを了知し、また、出力ポート情報は“CPU”であることから、パケット # 1 は CPU 2 0 によって処理されるべきものであることを了知し、パケット # 1 を CPU 2 0 に供給する。

【 0 0 7 4 】

その結果、CPU 2 0 は、パケット # 1 に対して所定の処理（例えば、ルーティング処理）を施した後、該当する入出力ポート（例えば、入出力ポート 1 2）から出力する。

【 0 0 7 5 】

続いて、パケット # 2 が入力された場合の動作について説明する。

パケット # 2 が入力された場合も、前述の場合と同様の処理が実行されるが、パケット # 2 は宛先 T C P ポート番号が 1 0 0 であるので、図 7 に示す参照テーブルの第 2 行目の情報に該当する。従って、出力ポート情報は存在しない（“－”である）ので、出力ポート情報セクタ 5 4 からは出力ポート情報は出力されず、また、フィルタ情報セクタ 5 5 からは“有”が出力される。

【 0 0 7 6 】

その結果、処理手段 3 0 は、パケット # 2 については破棄することになる。

以上の実施の形態によれば、入出力ポート 1 1 に接続されているインターネット 4 2 から、ホスト 4 3 の所定の T C P のポートに対してアクセスがなされた場合には、C P U 2 0 の判断を仰ぐことなく、パケットを破棄することが可能になるので、C P U 2 0 にかかる負担を増大することなく、フィルタリング処理を実行できる。

【 0 0 7 7 】

次に、図 1 0 に示すテーブルが参照テーブル 3 3 c に格納されている場合に、図 1 1 に示すパケット # 1 およびパケット # 2 がホスト 4 3 からパケット転送装置 4 0 に入力された場合の動作について説明する。

【 0 0 7 8 】

まず、パケット # 1 がパケット転送装置 4 0 に入力されると、入出力ポート 1 2 を介してパケットが取り込まれ、処理手段 3 1 に供給される。

処理手段 3 1 では、2 層ヘッダ情報抽出回路 3 0 a、3 層ヘッダ情報抽出回路 3 0 b、および、4 層ヘッダ情報抽出回路 3 0 c が、パケット # 1 からそれぞれ 2 層～4 層のヘッダ情報を抽出する。

【 0 0 7 9 】

いまの例では、2 層ヘッダ情報抽出回路 3 0 a は、宛先 M A C アドレス “m p a # 2” および送信元 M A C アドレス “m p a # 1” を抽出し、3 層ヘッダ情報抽出回路 3 0 b は、送信元 I P アドレス “p a # 1” および宛先 I P アドレス “p a # 2” を抽出し、また、4 層ヘッダ情報抽出回路 3 0 c は、送信元 T C P ポ

ート番号“x”および宛先TCPポート番号“100”を抽出する。

【0080】

2層ヘッダ情報抽出回路30a～4層ヘッダ情報抽出回路30cによって抽出された2層～3層ヘッダ情報は、参照ブロックインターフェース30dを介してテーブル33に供給される。

【0081】

いまの例では、参照テーブル33cに図10に示す、複数のヘッダ情報を含むテーブルが格納されているので、テーブル33では、連結比較回路33bが参照テーブル33cに格納されている参照フィールドと、ヘッダ情報とを比較する。

【0082】

即ち、連結比較回路33bの情報連結回路50は、処理手段31から供給された2層～4層のヘッダ情報を取得し、3層および4層のヘッダ情報を抽出して連結した後、参照情報レジスタ51に供給する。

【0083】

参照情報レジスタ51は、情報連結回路50から供給された3層および4層のヘッダ情報を一時的に格納するとともに参照テーブル33cに供給する。

参照テーブル33cは、参照情報レジスタ51から供給されたヘッダ情報と、参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドに格納されている制御情報を取得し、バス60を介して、出力ポート情報は出力ポート情報セクタ54に、また、フィルタ情報はフィルタ情報セクタ55に供給する。

【0084】

いまの例では、パケット#1のヘッダ情報は、図10に示す参照テーブルの第1行目の情報と一致するので、データフィールドから出力ポート情報として“ポート13”が、また、フィルタ情報として“無”が取得され、“ポート13”は出力ポート情報セクタ54に、また、“無”はフィルタ情報セクタ55に供給される。

【0085】

ここで、それ以外の参照テーブル33d、33eからの情報は存在しないので

、出力ポート情報セレクタ 5 4 およびフィルタ情報セレクタ 5 5 は、出力ポート情報 “ポート 1 3” およびフィルタ情報 “無” を、要求を行った処理手段 3 1 に供給する。

【 0 0 8 6 】

処理手段 3 1 は、参照ブロックインターフェース 3 0 d を介してこれらの情報を受信する。そして、フィルタ情報は “無” であることから、フィルタ処理は不要であることを了知し、また、出力ポート情報は “ポート 1 3” であることから、パケット # 1 は入出力ポート 1 3 から出力されるべきものであることを了知し、スイッチブロック 1 7 に供給する。

【 0 0 8 7 】

スイッチブロック 1 7 は、パケット # 1 を内蔵されているバッファに一旦格納した後、処理手段 3 2 に供給する。

処理手段 3 2 は、供給されたパケット # 1 を入出力ポート 1 3 を介して出力する。

【 0 0 8 8 】

その結果、パケット # 1 はホスト 4 4 に転送されることになる。

次に、パケット # 2 が入力された場合の動作について説明する。

パケット # 2 が入力された場合も、前述の場合と同様の処理が実行されるが、パケット # 2 は宛先ポート番号が 1 0 0 であるので、図 1 0 に示す参照テーブルの第 2 行目の情報に該当する。この場合、出力ポート情報は存在しない（ “ - ” である）ので、出力ポート情報セレクタ 5 4 からは出力ポート情報は出力されず、また、フィルタ情報セレクタ 5 5 からは “有” が出力される。

【 0 0 8 9 】

その結果、処理手段 3 1 は、パケット # 2 については破棄することになる。

以上の処理によれば、3 層および 4 層の情報に基づいてルーティングではなく、スイッチを行っている事になるので、MAC アドレスの付け替えが不要となり、それに付随する処理を省略することができるので、装置の構成を簡略化することが可能になる。

【 0 0 9 0 】

また、フィルタリング処理を処理手段のレベルで実行するようにしたので、CPU 20の判断を仰ぐことなくフィルタリングができるので、CPU 20の負担を軽減することが可能になる。

【0091】

次に、図12に示すテーブルが参照テーブル33cに格納され、また、図13に示すテーブルが参照テーブル33dに格納されている場合に、図14に示すパケット#1およびパケット#2がインターネット42からパケット転送装置40に入力された場合の動作について説明する。

【0092】

まず、パケット#1がパケット転送装置40に入力されると、入出力ポート11を介してパケットが取り込まれ、処理手段30に供給される。

処理手段30では、2層ヘッダ情報抽出回路30a、3層ヘッダ情報抽出回路30b、および、4層ヘッダ情報抽出回路30cが、パケット#1からそれぞれ2層～4層のヘッダ情報を抽出する。

【0093】

いまの例では、2層ヘッダ情報抽出回路30aは、宛先MACアドレス“ma#1”および送信元MACアドレス“ma#2”を抽出し、3層ヘッダ情報抽出回路30bは、送信元IPアドレス“pa#4”および宛先IPアドレス“pa#1”を抽出し、また、4層ヘッダ情報抽出回路30cは、送信元TCPポート番号“x”および宛先TCPポート番号“110”を抽出する。

【0094】

2層ヘッダ情報抽出回路30a～4層ヘッダ情報抽出回路30cによって抽出された2層～4層ヘッダ情報は、参照ブロックインターフェース30dを介してテーブル33に供給される。

【0095】

いまの例では、参照テーブル33cに図12に示すテーブルが格納され、また、参照テーブル33dに図13に示すテーブルが格納されており、それぞれ異なる層に属するヘッダ情報を含んでいることから、テーブル33では、連結比較回路33bが参照テーブル33cおよび参照テーブル33dのそれぞれの参照フィ

ールドと、ヘッダ情報とを比較する。

【0096】

即ち、連結比較回路33bの情報連結回路50は、処理手段30から供給された2層～4層のヘッダ情報から、送信元IPアドレスおよび宛先IPアドレスを抽出して参照情報レジスタ51に供給し、また、送信元IPアドレス、宛先IPアドレス、送信元TCPポート番号、および、宛先TCPポート番号を抽出して参照情報レジスタ52に供給する。

【0097】

参照情報レジスタ51および参照情報レジスタ52は、情報連結回路50から供給されたヘッダ情報を一時的に格納するとともに参照テーブル33cおよび参照テーブル33dにそれぞれ供給する。

【0098】

参照テーブル33cは、参照情報レジスタ51から供給されたヘッダ情報と、参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドに格納されている制御情報を取得し、バス60を介して、出力ポート情報は出力ポート情報セクタ54に、また、フィルタ情報はフィルタ情報セクタ55に供給する。

【0099】

参照テーブル33dも同様に、参照情報レジスタ52から供給されたヘッダ情報と、参照フィールドとを比較し、該当するデータが存在する場合にはデータフィールドに格納されている制御情報を取得し、バス60を介して、出力ポート情報は出力ポート情報セクタ54に、また、フィルタ情報はフィルタ情報セクタ55に供給する。

【0100】

いまの例では、パケット#1のヘッダ情報は、図12に示す参照テーブルの第1行目の情報と一致するので、データフィールドから出力ポート情報として“ポート12，13”が、また、フィルタ情報として“無”が取得され、“ポート12，13”は出力ポート情報セクタ54に、また、“無”はフィルタ情報セクタ55に供給される。

【 0 1 0 1 】

また、パケット # 1 のヘッダ情報は、図 1 3 に示す参照テーブルの第 1 行目の情報と一致するので、データフィールドから出力ポート情報として“ポート 1 3”が、また、フィルタ情報として“無”が取得され、“ポート 1 3”は出力ポート情報セクタ 5 4 に、また、“無”はフィルタ情報セクタ 5 5 に供給される。

【 0 1 0 2 】

ここで、出力ポート情報セクタ 5 4 は、参照テーブル 3 3 c から供給された出力ポート情報と、参照テーブル 3 3 d から供給された出力ポート情報とが異なっているので、より高い層のヘッダ情報を含む参照テーブルである参照テーブル 3 3 d からの出力ポート情報である“ポート 1 3”を選択し、処理手段 3 1 に供給する。

【 0 1 0 3 】

また、フィルタ情報セクタ 5 5 は、参照テーブル 3 3 c および参照テーブル 3 3 d から供給されたフィルタ情報の双方が“無”であることから、フィルタ情報として“無”を処理手段 3 1 に供給する。

【 0 1 0 4 】

処理手段 3 1 は、参照ブロックインターフェース 3 0 d を介してこれらの情報を受信する。そして、フィルタ情報は“無”であることから、フィルタ処理は不要であることを了知し、また、出力ポート情報は“ポート 1 3”であることから、パケット # 1 は入出力ポート 1 3 から出力されるべきものであることを了知し、スイッチブロック 1 7 に供給する。

【 0 1 0 5 】

スイッチブロック 1 7 は、内蔵されているバッファにパケット # 1 を一旦格納した後、処理手段 3 2 に供給する。

処理手段 3 2 は、供給されたパケット # 1 を入出力ポート 1 3 を介して出力する。

【 0 1 0 6 】

以上の処理の結果、パケット # 1 はホスト 4 4 に転送されることになる。

次に、パケット # 2 が入力された場合の動作について説明する。

パケット # 2 が入力された場合も、前述の場合と同様の処理が実行されるが、パケット # 2 は宛先 I P アドレスが “p a # 2” であり、また、宛先 I P アドレスが “p a # 1” であるので、参照テーブル 3 3 c からは出力ポート情報として “ポート 1 3” が、フィルタ情報として “有” が取得される。

【0 1 0 7】

また、送信元 I P アドレスは “p a # 4” であり、宛先 I P アドレスは “p a # 2” であり、宛先 T C P ポート番号は “1 0 0” であるので、参照テーブル 3 3 d からは出力ポート情報として “ポート 1 3” が、フィルタ情報として “無” が取得されることになる。

【0 1 0 8】

ここで、出力ポート情報セクタ 5 4 は、参照テーブル 3 3 c から供給された出力ポート情報と、参照テーブル 3 3 d から供給された出力ポート情報の双方が “ポート 1 3” であり、一致しているので、“ポート 1 3” を処理手段 3 1 に供給する。

【0 1 0 9】

また、フィルタ情報セクタ 5 5 は、参照テーブル 3 3 c から供給されたフィルタ情報は “有” であり、参照テーブル 3 3 d から供給されたフィルタ情報は “無” であり、一致していない。しかし、何れかの参照テーブルが “有” を指定している場合には、そのパケットは廃棄した方がセキュリティを向上させるという観点からは妥当である。そこで、フィルタ情報として “有” を処理手段 3 1 に供給する。

【0 1 1 0】

処理手段 3 1 は、フィルタ情報が “有” であるので、パケット # 2 は転送せずに廃棄することになる。

以上の処理によれば、複数の参照テーブルを設定し、出力ポート情報については最も高い層のヘッダ情報を参照フィールドに含む参照テーブルからの出力を選択し、フィルタ情報については何れかの参照テーブルから “有” が出力された場合にはフィルタリング処理を実行するようにしたので、フィルタリング処理につ

いては複数の設定のうち、何れかひとつにでも該当する場合にはパケットを廃棄することが可能になるので、セキュリティを向上させることが可能になるとともに、ネットワーク上を流れるパケットを有効に減少させることが可能になる。

【 0 1 1 1 】

また、出力ポート情報については、最も層が高いヘッダ情報を参照フィールドに含む参照テーブルの情報を選択するようにしたので、アプリケーションプログラムに近いレベルでのパケットの転送制御が可能になる。

【 0 1 1 2 】

なお、以上の実施の形態では、複数の層に属するヘッダ情報が参照フィールドに含まれている参照テーブルを例として説明したが、例えば、図 1 5 に示すように、単一の層に属するヘッダ情報のみが参照フィールドに格納されているテーブルを複数の参照テーブルに格納することも可能である。

【 0 1 1 3 】

図 1 5 (A) は I P アドレスのみが参照フィールドに格納されている例であり、また、図 1 5 (B) は T C P ポート番号のみが参照フィールドに格納されている例である。具体的には、図 1 5 (A) には、宛先 I P アドレスと入出力ポート番号とが対応付けて格納されている。また、図 1 5 (B) には、宛先 T C P ポート番号と、入出力ポート番号とが対応付けて格納されている。

【 0 1 1 4 】

このような単一のヘッダ情報を参照フィールドに含むテーブルを用いた場合でも、参照テーブルから出力される制御情報を、一定のルールに基づいて選択するようにすれば、前述のような複数のヘッダ情報を含む参照テーブルと同様の機能を実現することが可能になる。

【 0 1 1 5 】

次に、図 1 6 を参照して、連結比較回路 3 3 b において実行される処理について説明する。このフローチャートが開始されると、以下のステップが実行される。

【 0 1 1 6 】

ステップ S 1 1 :

パケットが供給された入出力ポートは、パケットを受信し、処理手段に供給する。

【0 1 1 7】

ステップ S 1 2 :

処理手段の 2 層ヘッダ抽出回路～4 層ヘッダ抽出回路は、2 層～4 層のヘッダ情報を抽出し、連結比較回路 3 3 b に供給する。

【0 1 1 8】

ステップ S 1 3 :

連結比較回路 3 3 b は、供給されたヘッダ情報を連結して参照情報レジスタ 5 1 ～5 3 に供給し、その結果として参照テーブル 3 3 c ～3 3 e から出力される制御情報を取得する。

【0 1 1 9】

ステップ S 1 4 :

フィルタ情報セクタ 5 5 は、制御情報のうちフィルタ情報を抽出する。

ステップ S 1 5 :

フィルタ情報セクタ 5 5 は、複数のセクタ情報が存在する場合には、“有” が 1 つ以上存在するか否かを判定し、1 つ以上存在する場合にはステップ S 1 6 に進み、それ以外の場合にはステップ S 1 7 に進む。

【0 1 2 0】

ステップ S 1 6 :

パケットを受信した処理手段は、フィルタ処理によりパケットを破棄する。

ステップ S 1 7 :

出力ポート情報セクタ 5 4 は、制御情報から出力ポート情報を抽出する。

【0 1 2 1】

ステップ S 1 8 :

出力ポート情報セクタ 5 4 は、出力ポート情報が複数存在する場合には、これらが不一致であるか否かを判定し、不一致である場合にはステップ S 1 9 に進み、それ以外の場合にはステップ S 2 0 に進む。

【0 1 2 2】

ステップ S 1 9 :

出力ポート情報セクタ 5 4 は、参照フィールドに最上層のヘッダ情報を含む参照テーブルの出力ポート情報を選択する。

【 0 1 2 3 】

ステップ S 2 0 :

パケットを受信した処理手段は、パケットを対応するスイッチブロック 1 7 に供給する。その結果、スイッチブロック 1 7 は、指定された入出力ポートからパケットを出力させる。

【 0 1 2 4 】

このようなフローチャートによれば、上述した機能を実現することが可能になる。

以上に説明したように、本実施の形態では、パケットから 2 層に属する情報のみならず、3 層以上に属するヘッダ情報も抽出し、参照テーブルと比較することにより、そのパケットの制御内容を決定するようにしたので、CPU 2 0 の負担を増大することなく、入出力ポート、端末、および、パケット毎に細かな通信ポリシーを設定することが可能になるので、柔軟でしかもセキュリティの高いシステムを構築することが可能になる。

【 0 1 2 5 】

なお、以上の実施の形態では、MAC アドレスを参照テーブルに登録しないようにしたが、MAC アドレスを登録する事も可能である。その場合、例えば、家庭内または S O H O 側に属する MAC アドレスがインターネット側から入力されてきた場合には、これをフィルタリングするようにすれば、外部に漏洩した MAC アドレスを利用して第三者が成りすましにより進入することを防止することが可能になる。

【 0 1 2 6 】

また、受信ポート情報を合わせて参照できるようにすると、プライベートアドレスを使用した WAN 側からのなりすましなどに対処できるようになる。

また、家庭内または S O H O 側の端末に対して外部からコネクションを張りに来るパケットを識別できるように、TCP ヘッダ内の SYN や ACK フラグを参

照テーブルに追加し、このようなフラグが立っているパケットをフィルタリングすることも可能である。

【 0 1 2 7 】

更に、図 3 に示すレイヤ 2 スイッチ 1 0 を I C 化して半導体装置として構成することも可能である。なお、その際、C P U 2 0 については同一のチップ上に併せて構成するようにしてもよいし、別チップとしてもよい。

【 0 1 2 8 】

(付記 1) 複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層 (ネットワーク層) 以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とするパケット転送装置。

【 0 1 2 9 】

(付記 2) 前記制御情報は、パケットに対するフィルタリング処理の有無を示し、

前記処理手段は、前記制御情報がフィルタリングが必要であることを指示している場合には、当該パケットを破棄する、

ことを特徴とする付記 1 記載のパケット転送装置。

【 0 1 3 0 】

(付記 3) 外部のネットワークに接続された入出力ポートを有し、

前記処理手段は、前記外部のネットワークに接続された入出力ポートから入力されたパケットが、内部の装置のアドレス情報を有している場合には、これをフィルタリングすることを特徴とする付記 2 記載のパケット転送装置。

【 0 1 3 1 】

（付記 4） 前記制御情報は、前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報であり、

前記処理手段は、前記制御情報に基づいて、指定された入出力ポートから当該パケットを出力する、

ことを特徴とする付記 1 記載のパケット転送装置。

【 0 1 3 2 】

（付記 5） 前記テーブルには、異なる階層に属する複数のヘッダ情報と、当該複数のヘッダ情報に対応する制御情報とが対応付けて格納されていることを特徴とする付記 1 記載のパケット転送装置。

【 0 1 3 3 】

（付記 6） 異なる情報が格納された複数のテーブルを有することを特徴とする付記 1 記載のパケット転送装置。

（付記 7） 前記制御情報取得手段によって、複数のテーブルから複数の制御情報が 1 つのパケットに対して取得された場合には、前記処理手段が実際に実行すべき処理を決定する処理決定手段を更に有することを特徴とする付記 1 記載のパケット転送装置。

【 0 1 3 4 】

（付記 8） 前記制御情報は、パケットに対するフィルタリングの有無を示し

前記処理決定手段は、前記複数のテーブルから複数の制御情報が取得された場合に何れか 1 つの制御情報がフィルタリングが必要であることを指示している場合には、当該パケットを破棄する、

ことを特徴とする付記 7 記載のパケット転送装置。

【 0 1 3 5 】

（付記 9） 前記制御情報は、前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報であり、

前記処理決定手段は、前記複数のテーブルから複数の制御情報が取得された場合には、最も階層が高いヘッダ情報を含むテーブルから取得された制御情報によ

って指定される入出力ポートから当該パケットを出力する、

ことを特徴とする付記 7 記載のパケット転送装置。

【 0 1 3 6 】

(付記 1 0) 前記制御情報は、前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報およびパケットに対するフィルタリングの有無を示す情報の双方を含み、

前記処理決定手段は、前記複数のテーブルから前記複数の入出力ポートのいずれから当該パケットを出力するかを指定する情報およびパケットに対するフィルタリングの有無を示す情報の双方が取得された場合には、当該パケットを破棄することを決定する、

ことを特徴とする付記 7 記載のパケット転送装置。

【 0 1 3 7 】

(付記 1 1) ルーティング処理を実行するルーティング処理手段を更に有することを特徴とする付記 1 記載のパケット転送装置。

(付記 1 2) 前記テーブルの内容を書き換えるテーブル書き換え手段を更に有することを特徴とする付記 1 記載のパケット転送装置。

【 0 1 3 8 】

(付記 1 3) 複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層 (ネットワーク層) 以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とする半導体装置。

【 0 1 3 9 】

(付記 1 4) 複数のネットワークがパケット転送装置によって接続され、それぞれのネットワーク間でパケットを転送するパケット転送システムにおいて、

前記パケット転送装置は、

複数の入出力ポートと、

前記複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層 (ネットワーク層) 以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、

ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、

前記ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報を前記テーブルから取得する制御情報取得手段と、

前記制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、

を有することを特徴とするパケット転送システム。

【 0 1 4 0 】

【発明の効果】

以上説明したように本発明では、複数の入出力ポートと、複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層 (ネットワーク層) 以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報をテーブルから取得する制御情報取得手段と、制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、を設けるようにしたので、通信ポリシーをパケット単位および入出力ポート単位で設定できるので、柔軟なシステムを構成することが可能になる。

【 0 1 4 1 】

また、複数の入出力ポートと、複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層 (ネットワーク層) 以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、ヘッダ情報と、当該ヘッダ情報に

対応する制御情報とを関連付けて記憶したテーブルと、ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報をテーブルから取得する制御情報取得手段と、制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、を設けるようにしたので、CPUにかかる負担を軽減することにより、装置全体の処理速度を向上させることが可能になる。

【0142】

また、複数のネットワークがパケット転送装置によって接続され、それぞれのネットワーク間でパケットを転送するパケット転送システムにおいて、パケット転送装置は、複数の入出力ポートと、複数の入出力ポートのそれぞれから入力されたパケットより、ネットワークプロトコルの3層（ネットワーク層）以上に属するヘッダ情報を抽出するヘッダ情報抽出手段と、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶したテーブルと、ヘッダ情報抽出手段によって抽出されたヘッダ情報に対応する制御情報をテーブルから取得する制御情報取得手段と、制御情報取得手段によって取得された制御情報に基づいて、パケットを処理する処理手段と、を有するようにしたので、通信ポリシーをパケット単位および入出力ポート単位で設定できるので、柔軟なシステムを構成することが可能になる。

【図面の簡単な説明】

【図1】

本発明の動作原理を説明する原理図である。

【図2】

本発明の実施の形態の構成例を示す図である。

【図3】

図2に示すパケット転送装置の詳細な構成例を示す図である。

【図4】

図3に示す処理手段と参照ブロックの詳細な構成例を示す図である。

【図5】

図4に示す連結比較回路の詳細な構成例を示す図である。

【図6】

参照テーブルに格納されているテーブルの一例である。

【図 7】

参照テーブルに格納されているテーブルの一例である。

【図 8】

パケットに含まれているヘッダ情報の一例である。

【図 9】

パケットに含まれているヘッダ情報の配置例である。

【図 1 0】

参照テーブルに格納されているテーブルの一例である。

【図 1 1】

パケットに含まれているヘッダ情報の一例である。

【図 1 2】

参照テーブルに格納されているテーブルの一例である。

【図 1 3】

参照テーブルに格納されているテーブルの一例である。

【図 1 4】

パケットに含まれているヘッダ情報の一例である。

【図 1 5】

参照テーブルに格納されているテーブルの一例である。

【図 1 6】

連結比較回路において実行される処理を説明するフローチャートである。

【図 1 7】

従来のアクセスルータの構成例を示す図である。

【図 1 8】

図 1 7 に示す参照ブロックおよび処理手段の構成例を示す図である。

【図 1 9】

図 1 8 に示す参照テーブルに格納されているテーブルの一例である。

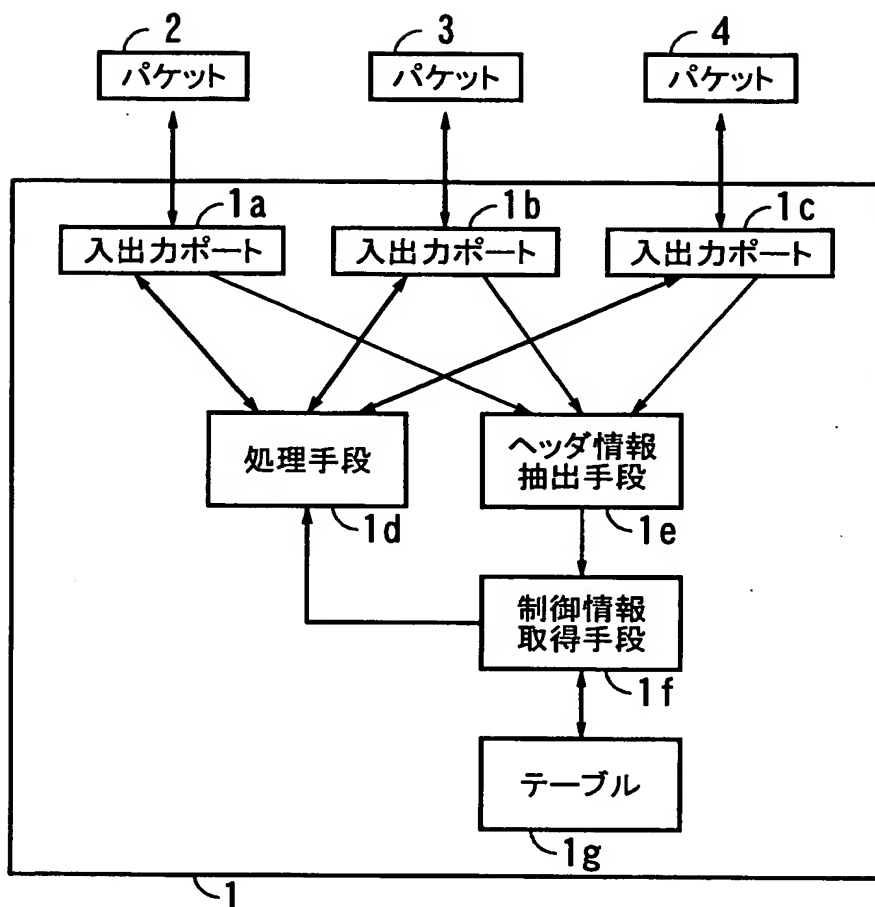
【符号の説明】

1 パケット転送装置

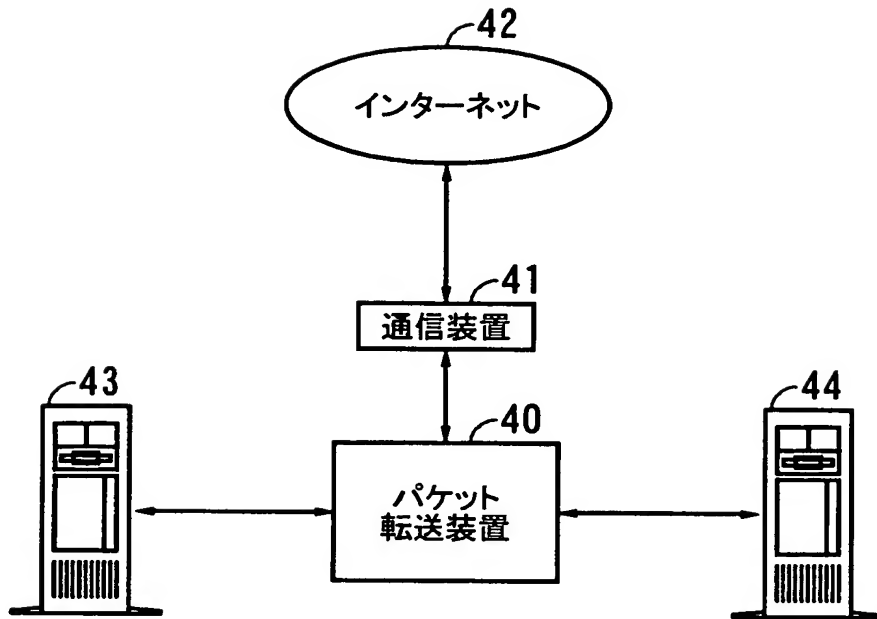
- 1 a ~ 1 c 入出力ポート
- 1 d 処理手段
- 1 e ヘッダ情報抽出手段
- 1 f 制御情報取得手段
- 1 g テーブル
- 2 ~ 4 パケット
- 1 0 レイヤ 2 スイッチ
- 1 1 ~ 1 3 入出力ポート
- 1 7 スイッチブロック
- 2 0 C P U
- 3 0 ~ 3 2 処理手段
- 3 3 テーブル
- 4 0 パケット転送装置
- 4 1 通信装置
- 4 2 インターネット
- 4 3, 4 4 ホスト
- 3 0 a 2 層ヘッダ情報抽出回路
- 3 0 b 3 層ヘッダ情報抽出回路
- 3 0 c 4 層ヘッダ情報抽出回路
- 3 0 d 参照ブロックインターフェース
- 3 0 e スイッチブロックインターフェース
- 3 3 a 比較回路
- 3 3 b 連結比較回路
- 3 3 c ~ 3 3 e 参照テーブル
- 5 0 情報連結回路
- 5 1 ~ 5 3 参照情報レジスタ
- 5 4 出力ポート情報セレクタ
- 5 5 フィルタ情報セレクタ
- 6 0 バス

【書類名】 図面

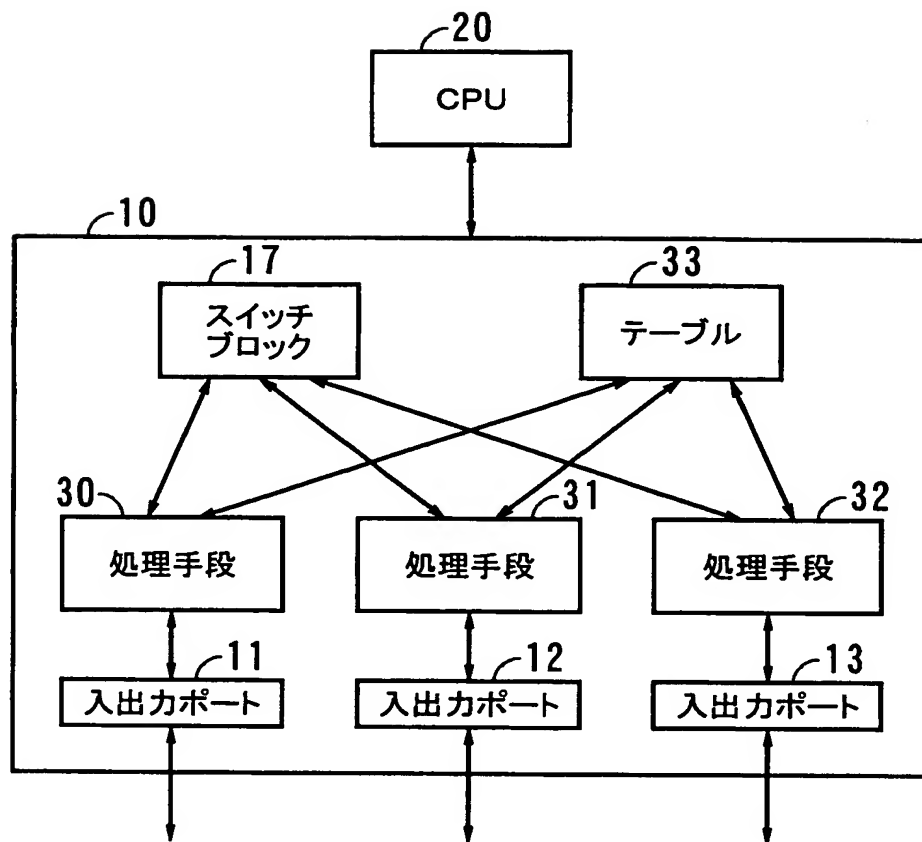
【図 1】



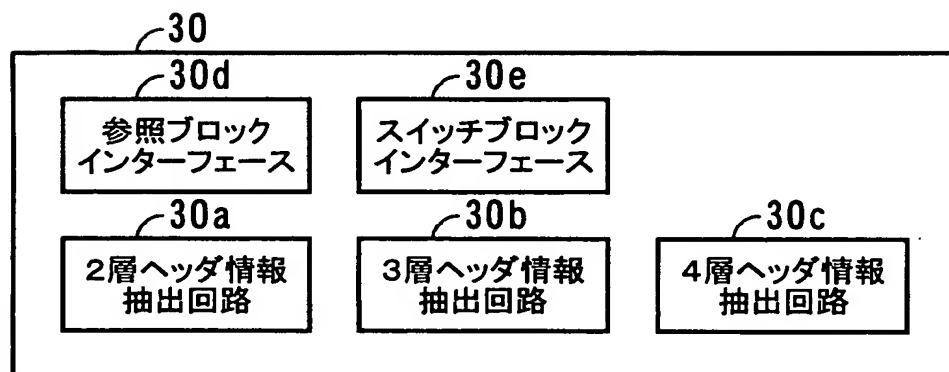
【図 2】



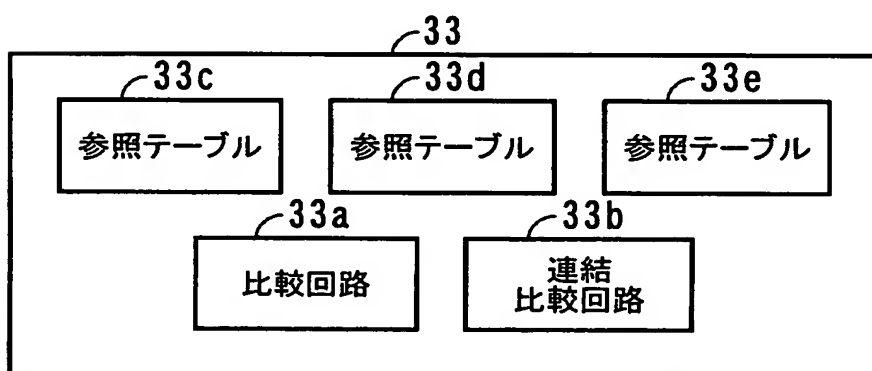
【図3】



【図 4】

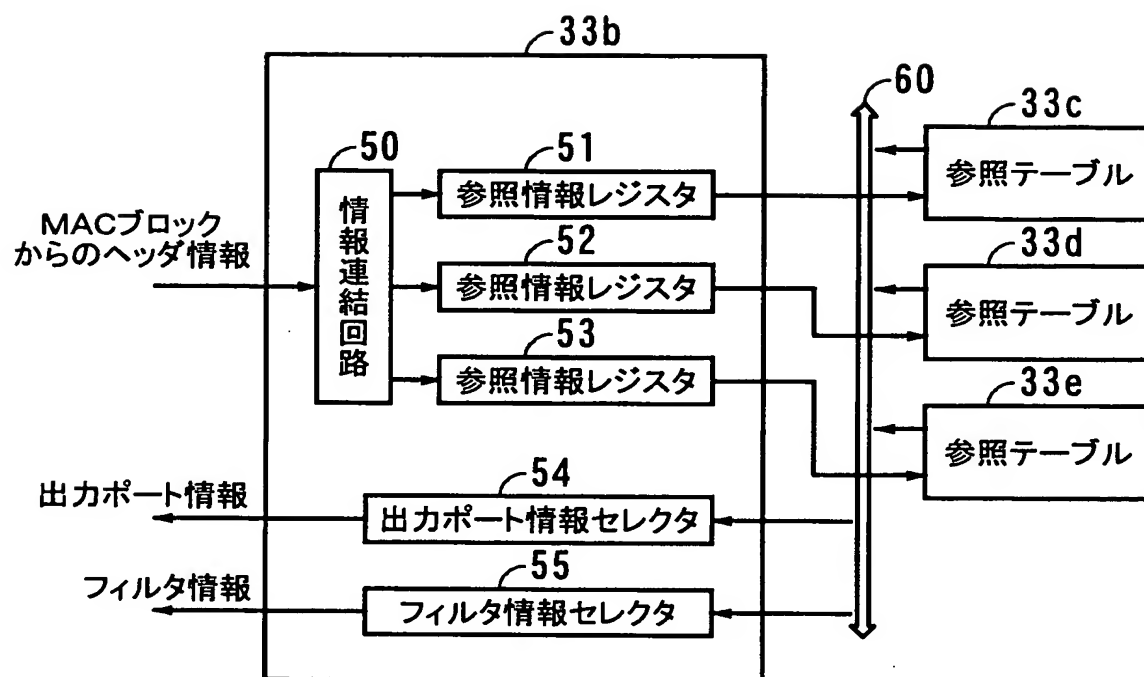


(A)



(B)

【図 5】



【図 6】

参照フィールド				データフィールド		
送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号	入出力ポート	フィルタ有無	
SA#1	DA#1	SP#1	DP#1	P#1	無	
SA#2	DA#2	SP#2	DP#2	P#2	無	
SA#3	DA#3	SP#3	DP#3	—	有	

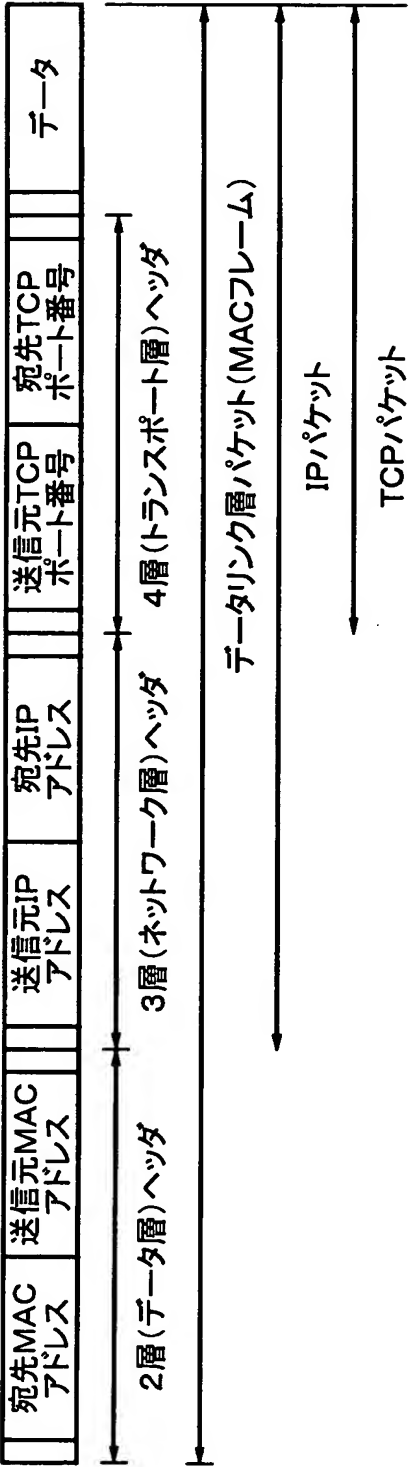
【図 7】

参照フィールド				データフィールド		
受信 入出力ポート	送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号	入出力ポート	フィルタ有無
ポート11	gaany	ga#1	tcpany	80	CPU	無
ポート11	gaany	ga#1	tcpany	100	—	有
.
.
.

【図 8】

	宛先MAC アドレス	送信元MAC アドレス	送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号
パケット#1	ma#1	max	gax	ga#1	x	80
パケット#2	ma#1	max	gax	ga#1	x	100
.
.
.

【図 9】



【図 1 0】

参照フィールド				データフィールド	
送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号	入出力ポート	フィルタ有無
pa#1	pa#2	tcpany	110	ポート13	無
pa#1	pa#2	tcpany	100	—	有
.
.
.

【図 1 1】

	宛先MAC アドレス	送信元MAC アドレス	送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号
パケット#1	mpa#2	mpa#1	pa#1	pa#2	x	110
パケット#2	mpa#2	mpa#1	pa#1	pa#2	x	100
.
.
.

【図 1 2】

参照フィールド		データフィールド	
送信元IP アドレス	宛先IP アドレス	入出力ポート	フィルタ有無
pa#4	pa#1	ポート12, 13	無
pa#4	pa#2	ポート13	有
.	.	.	.
.	.	.	.
.	.	.	.

【図 1 3】

参照フィールド			データフィールド		
送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号	入出力ポート	フィルタ有無
pa#4	pa#1	x	110	ポート13	無
pa#4	pa#2	x	100	ポート13	無
.
.
.

【図 1 4】

	宛先MAC アドレス	送信元MAC アドレス	送信元IP アドレス	宛先IP アドレス	送信元TCP ポート番号	宛先TCP ポート番号
パケット#1	ma#1	ma#2	pa#4	pa#1	x	110
パケット#2	ma#1	ma#2	pa#4	pa#2	x	100
.
.
.

【図 1 5】

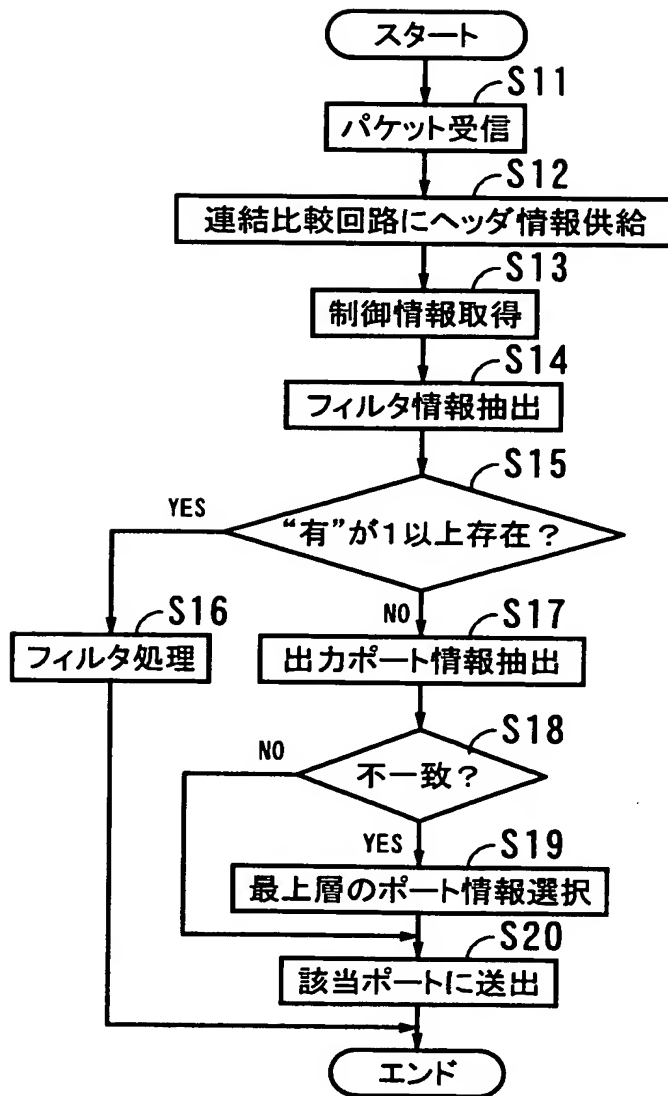
参照フィールド	データフィールド
IPアドレス#1	ポート11
IPアドレス#2	ポート12
IPアドレス#3	ポート13

(A)

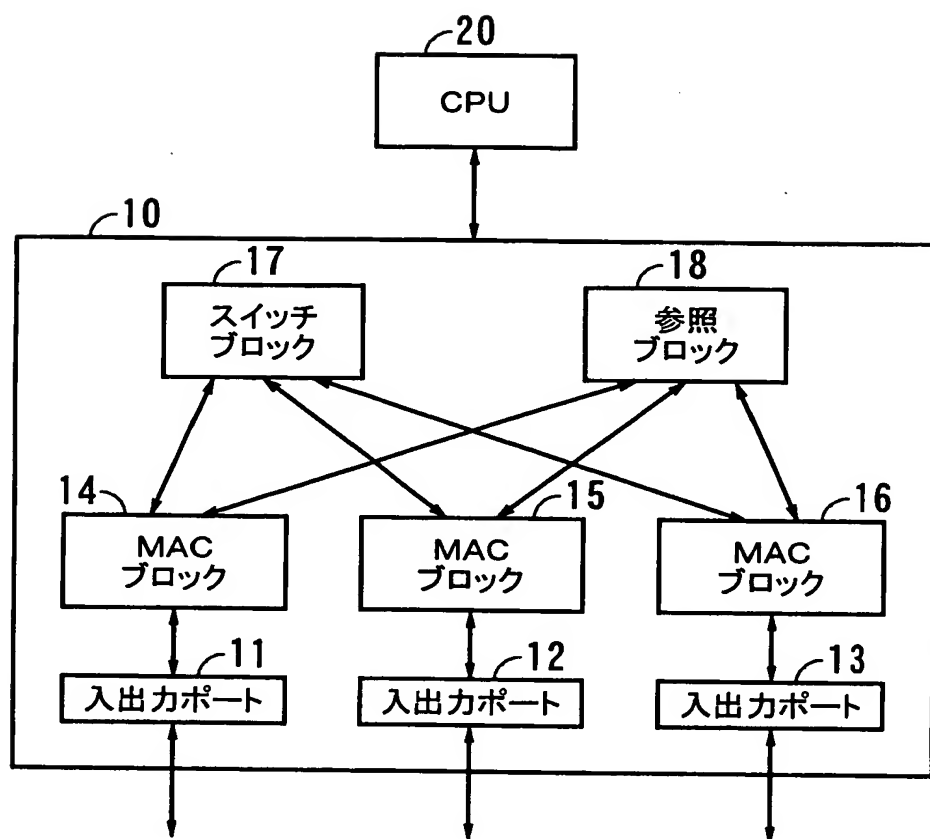
参照フィールド	データフィールド
TCPポート#1	ポート11
TCPポート#2	ポート12
TCPポート#3	ポート13

(B)

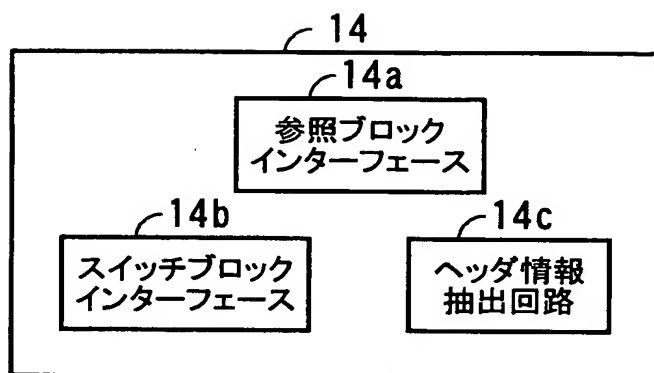
【図 1 6】



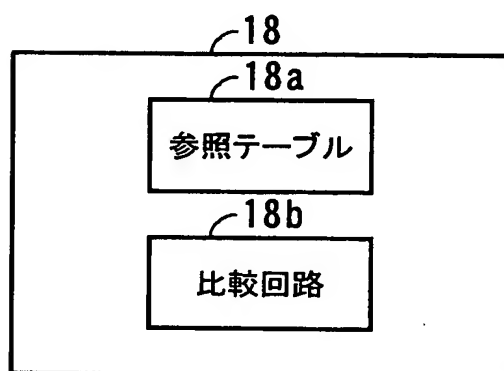
【図 1 7】



【図 1 8】



(A)



(B)

【図 1 9】

参照フィールド	データフィールド
MACアドレス#1	ポート番号#1
MACアドレス#2	ポート番号#2
MACアドレス#3	ポート番号#3

【書類名】 要約書

【要約】

【課題】 レイヤ 2 スイッチを有するパケット転送装置において 3 層以上のヘッダ情報を参照してスイッチングする。

【解決手段】 入出力ポート 1 a ～ 1 c は、パケット転送装置に接続された他の装置との間でパケットを授受する。ヘッダ情報抽出手段 1 e は、複数の入出力ポート 1 a ～ 1 c のそれぞれから入力されたパケットより、ネットワークプロトコルの 3 層（ネットワーク層）以上に属するヘッダ情報を抽出する。テーブル 1 g は、ヘッダ情報と、当該ヘッダ情報に対応する制御情報とを関連付けて記憶している。制御情報取得手段 1 f は、ヘッダ情報抽出手段 1 e によって抽出されたヘッダ情報に対応する制御情報をテーブル 1 g から取得する。処理手段 1 d は、制御情報取得手段 1 f によって取得された制御情報に基づいて、パケットを処理する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日
[変更理由] 住所変更
住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
氏 名 富士通株式会社